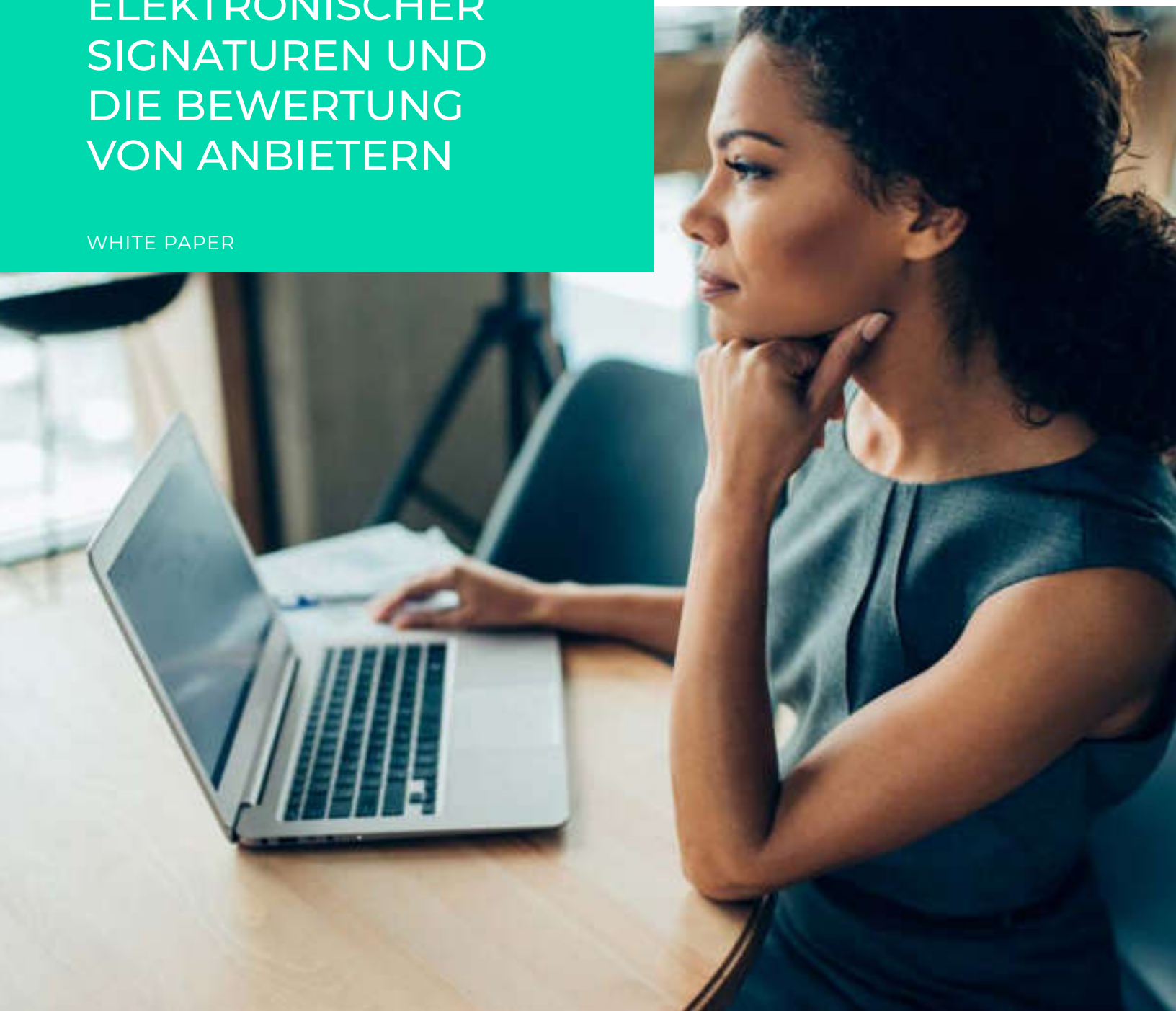
OneSpan
Be bold. Be secure.

SICHERHEIT UND VERTRAUEN: BEST PRACTICES FÜR DIE EINFÜHRUNG ELEKTRONISCHER SIGNATUREN UND DIE BEWERTUNG VON ANBIETERN

WHITE PAPER



INHALTSVERZEICHNIS

Best Practices für die Einführung elektronischer Signaturen und die Bewertung von Anbietern

Sicherheit ist verständlicherweise eines der wichtigsten Anliegen bei digitalen Transaktionen. Sie müssen sich daher vergewissern, dass Ihr Anbieter für digitale Signaturen die höchsten Sicherheitsstandards erfüllt, und eine vertrauensvolle Erfahrung zwischen Ihnen und Ihren Mitarbeitern und Kunden gewährleistet.

Dazu gehört viel mehr, als nur ein Sicherheitsaudit zu bestehen oder eine Zertifizierung zu erhalten. Um die Sicherheit von E-Signaturen zu gewährleisten, empfehlen wir einen breiten Ansatz, der insbesondere auch folgende Punkte berücksichtigt:

- Auswahl der geeigneten Autorisierungsebene
- Schutz der E-Signaturen und Dokumente vor Manipulation
- Erleichterte Überprüfung von elektronisch signierten Dokumenten
- Langfristige Zuverlässigkeit Ihrer elektronischen Dokumente – unabhängig vom Anbieter
- Gewissheit, dass der Anbieter eine konstante Erfolgsbilanz beim Schutz von Kundendaten vorzuweisen hat
- Durchgehend vertrauenswürdige Erfahrung durch White-Labeling und Integration in Ihre bestehende Identitäts- und Zugriffsverwaltung (IAM)

Indem Sie bei der Sicherheit elektronischer Signaturen einen differenzierten Ansatz verfolgen, stellen Sie sicher, dass Ihre Dokumente im Fall eines Rechtsstreits zuverlässig wiederhergestellt werden können.

Wenn Sie bei der Sicherheit elektronischer Signaturen einen differenzierten Ansatz verfolgen, stellen Sie sicher, dass Ihre Dokumente im Fall eines Rechtstreits zuverlässig wiederhergestellt werden können. Dieser Ansatz stärkt außerdem das Vertrauen der Kunden, schützt den Ruf Ihres Unternehmens, mindert das Risiko von Bußgeldern für Konformitätsverstöße, begrenzt die Abhängigkeit von einzelnen Anbietern und vieles mehr.

Dieses White Paper beantwortet für Sie folgende Fragen, die Sie bezüglich der Sicherheitsanforderungen für Ihre Lösungen abwägen sollten: Wie kann ich herausfinden, wer ein Dokument elektronisch signiert hat? Wie werden die E-Signaturen der Kunden geschützt? Wie leicht kann geprüft werden, ob ein elektronisch signiertes Dokument geändert wurde? Und wie kann ich beim Einsatz von E-Signaturen in der Cloud sicher sein, dass meine Kundendaten geschützt werden?

1. Identifizierung, Authentifizierung und Zuordnung

Gesetze zu E-Signaturen treffen kaum Aussagen im Hinblick auf Sicherheitsverfahren und -technologie, aber die rechtliche Definition einer elektronischen Signatur enthält immer Formulierungen rund um die Identität des Unterzeichners.

Das bedeutet, dass Unternehmen Maßnahmen ergreifen müssen, um Benutzer vor dem elektronischen Signieren zu identifizieren und/oder authentifizieren, und sie diese Authentifizierung mit der E-Signatur und dem elektronisch signierten Dokument verknüpfen müssen.

Die Authentifizierung von Benutzern und Transaktionen gehört zu den vorrangigen Aufgaben von Banken und anderen Unternehmen, die online oder mobil geschäftlich tätig sind.

Identifizierung

Bei der Überlegung, wie neue Kunden über das Internet identifiziert werden können, brauchen Sie nur daran denken, wie dies bereits anderweitig aus der Ferne geschieht – beispielsweise in Callcentern oder per Post. Bei diesen Verfahren werden neue Antragssteller meist anhand von zwei Arten von persönlichen Informationen identifiziert:

- Personenbezogene Daten
- Nicht-öffentliche persönliche Daten

Die Informationen des Kunden werden gewöhnlich durch einen externen Identifizierungsdienst (z. B. Experian, Trans Union, Equifax) geprüft. Beispielsweise nutzen Finanzdienstleiter häufig Dienste von Drittanbietern, da diese oft bereits im Rahmen von Darlehensanträgen und anderen Prozessen auf Kreditdatenbanken zugreifen. Achten Sie in diesem Fall darauf, dass sich in die E-Signatur-Lösung Identitätsprüfungsdienste von Drittanbietern integrieren lassen.

Authentifizierung

Sobald die Identität eines Unterzeichners geprüft wurde, stellen Unternehmen oft elektronische Anmeldedaten bereit, die zukünftige den Zugriff auf digitale Transaktionen ermöglichen. Im Fall von bestehenden Kunden ist es sehr zu empfehlen, möglichst Anmeldedaten zu nutzen, die Sie bereits ausgestellt haben (z. B. für die Anmeldung zum Online-Banking). Derartige Anmeldedaten sind nicht nur zuverlässig, wenn sie über lange Zeit verwendet wurden, sondern ersparen dem Kunden auch die Umstände, wieder ein neues Passwort zu erstellen und sich daran erinnern zu müssen.

Außerdem nutzen Unternehmen in bestimmten Regionen oder in Branchen, in denen Transaktionen mit hohem Wert und hohem Risiko gehandhabt werden, oft leistungsstarke Multi-Faktor-Authentifizierungsdienste (z. B. den Digipass von OneSpan®) während des Prozesses. Dies stärkt das Vertrauen in die Transaktion und schafft ein sicheres Umfeld, in dem Identitäten, Daten und das digitale Leben geschützt sind. Wählen Sie in diesem Fall eine E-Signatur- Lösung, die im Workflow des elektronischen Signierprozesses leicht Authentifizierungsdienste integrieren kann.

Der Unterschied zwischen digitalen und elektronischen Signaturen

Die Begriffe „E-Signatur“ und „digitale Signatur“ werden häufig verwechselt. Eine elektronische Signatur ist, wie auch das Äquivalent in Papierform, ein rechtliches Konzept. Ihr Zweck ist die Erfassung der Absicht einer Person, rechtlich an eine Vereinbarung oder einen Vertrag gebunden zu werden.

Eine digitale Signatur ist hingegen eine Sicherheitstechnologie. Basierend auf der Kryptographie mit einem öffentlichen/privaten Schlüssel werden digitale Signaturen in einer Vielzahl von Sicherheits-, E-Business- und E-Commerce-Anwendungen eingesetzt. Beim Einsatz in einer Anwendung zum elektronischen Unterzeichnen schützt die digitale Signaturverschlüsselung die elektronisch signierten Daten. Wenn ein elektronisch signiertes Dokument geändert oder gefälscht wird, erkennt dies die digitale Signaturtechnologie und macht das Dokument ungültig.

Anders als bei Verträgen und Unterschriften auf Papier, die eine sorgfältige Überprüfung durch das menschliche Auge erfordern, können bei elektronisch unterzeichneten Verträgen, die auf digitalen Signaturen beruhen, Fehler oder Änderungen automatisch erkannt werden. Digitale Signaturen sind daher die Grundlage jeder zuverlässigen Signatur und eine wesentliche Anforderung an eine vertrauenswürdige Lösung.

Obwohl es zahlreiche sichere und benutzerfreundliche Optionen zur Online-Identifizierung von Unterzeichnern gibt, hängt die Auswahl der Authentifizierungsmethode letztendlich vom Risikoprofil des zu automatisierenden Prozesses und der zugrundeliegenden digitalen Transaktion ab. Entscheidend dabei ist, die Benutzer zu authentifizieren, ohne ihr Erlebnis zu beeinträchtigen. Wählen Sie daher E-Signatur-Lösungen, die eine große Bandbreite an Authentifizierungsoptionen bieten, die Ihren Bedürfnissen entsprechen und so bessere Erlebnisse ermöglichen.

Zuordnung

Die Zuordnung von Signaturen bezeichnet den Vorgang, mit dem nachgewiesen wird, wer eigentlich zum Anbringen einer E-Signatur geklickt hat. Diese Fragen zur Zuordnung stellen sich oft bei Vorgängen, bei denen Mitarbeiter auf einem gemeinsamen Gerät mit Kunden mithilfe der Click-to-sign-Methode persönlich interagieren. So kann beispielsweise in einem Anwendungsfall ein Unterzeichner gebeten werden, einen Knopf auf dem Laptop eines Vertreters zu drücken, um elektronisch zu unterschreiben. Die Herausforderung besteht darin, den Nachweis zu erbringen, wer die Maus in der Hand hatte, als die E-Signatur angebracht wurde. In derartigen

Fällen gibt es zwei bewährte Ansätze zur Bestimmung der Zuordnung: eidesstattliche Versicherungen und der Einsatz von SMS-Passcodes, die an das persönliche Mobiltelefon gesendet werden.

Eidesstattliche Versicherungen sind die kostengünstigste und einfachste Möglichkeit, die Zuordnung zu bestimmen. Kurz bevor die Kontrolle über einen Laptop oder Tablet-Computer zum Signieren an den Kunden übergeben wird, wird Ihrem Mitarbeiter oder Vertreter ein Text einer eidesstattlichen Versicherung angezeigt, mit der dieser bestätigt, dass die Kontrolle an den Unterzeichner übergeben wird. Dieser Übergang der Kontrolle würde als Teil des Audit-Trails erfasst werden.

Eine andere Möglichkeit wäre, das persönliche Smartphone des Unterzeichners zu Hilfe zu nehmen. Per SMS-Textnachricht kann so einem Unterzeichner ein Passcode zum einmaligen Gebrauch zugeschickt werden, mit dem er Zugang zu einer E-Signatur-Sitzung erlangt.

2. Sicherheit von Dokumenten und Signaturen

Die Sicherheit von Dokumenten und Signaturen ist der Kernpunkt eines jeden elektronisch signierten Vertrags oder Dokuments. Dabei sind verschiedene Punkte zu berücksichtigen:

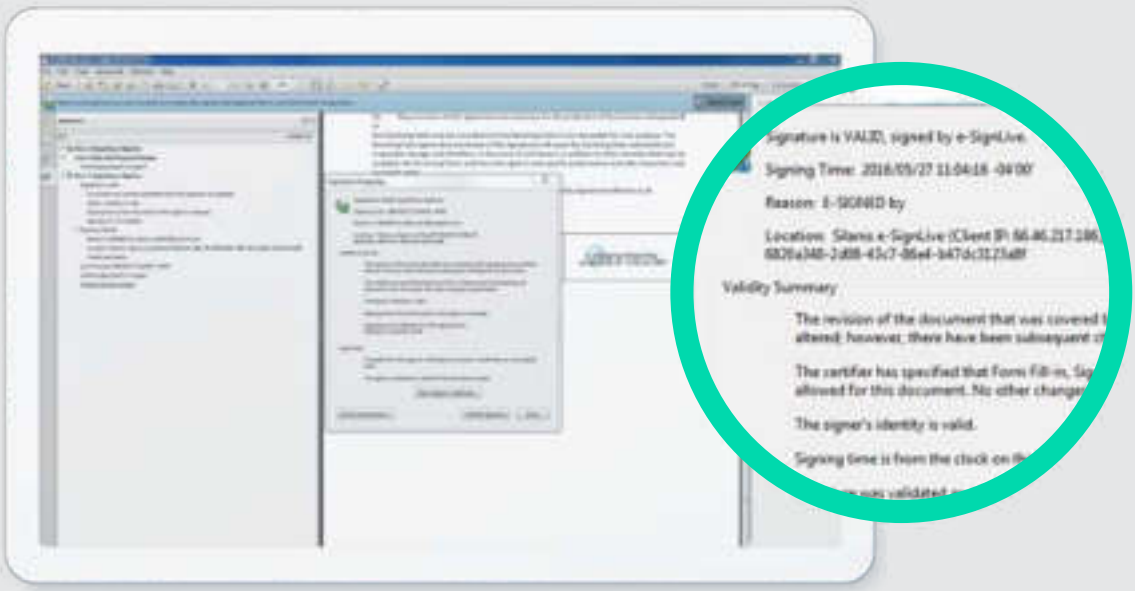
- Das Dokument und **alle** Signaturen müssen mit einer digitalen Signatur abgesichert werden, um das Dokument fälschungssicher zu machen und sicherzustellen, dass Signaturen nicht kopiert und eingefügt werden können
- Ein umfassendes Prüfprotokoll muss das Datum und die Uhrzeit jeder **einzelnen Signatur** enthalten
- Das Prüfprotokoll muss sicher im Dokument **eingebettet** und mit **jeder einzelnen** Signatur verknüpft sein
- Es muss – **unabhängig vom Anbieter** – leicht zu prüfen sein, dass am signierten Dokument keine Änderungen vorgenommen wurden
- Das Dokument muss **allen Beteiligten zugänglich** sein

Digitale Signaturtechnologie – an allen Signaturen

Das Dokument und jede einzelne elektronische Signatur muss mithilfe von digitaler Signaturtechnologie geschützt werden. Mit der digitalen Signatur wird ein digitaler Fingerabdruck des Dokuments (ein so genannter Hash) erstellt, mit dem später die Integrität des elektronischen Dokuments überprüft werden kann. Wurde das Dokument auch nur im Geringsten manipuliert, wird die elektronische Signatur sichtbar ungültig. Dies ist ein einzigartiger Vorteil gegenüber Signaturen auf Papier, denn Änderungen an einem Papierdokument sind nicht immer leicht zu erkennen. Vom Anbringen einer digitalen Signatur als Umschlag eines Dokuments (nachdem alle Signaturen erfasst wurden) wird abgeraten.

Das Dokument und die Signaturen sind während des Prozesses ungeschützt und die Datums- und Zeitstempel der einzelnen Signaturen sind falsch. Falls ein Unterzeichner und ein Mitunterzeichner ein Dokument an zwei verschiedenen Tagen elektronisch unterzeichnen, muss sich dieser Verlauf im Prüfprotokoll widerspiegeln. Optimal ist die digitale Signaturverschlüsselung nach Hinzufügen der jeweilige E-Signatur zum Dokument. Dadurch entsteht ein umfassendes Prüfprotokoll mit dem Datum und der Uhrzeit des Hinzufügens der jeweiligen Signatur.

Überprüfung von Dokumenten- und Signaturintegrität in OneSpan Sign



Detailliertes, im Dokument eingebettetes Prüfprotokoll

Alle elektronischen Signaturen, Zeitstempel und Prüfprotokolle sollten direkt in das Dokument eingebettet sein, anstatt separat in der Cloud gespeichert oder „logisch“ in einer Datenverwaltung oder proprietären Datenbank zugeordnet zu werden. Außer der größeren Sicherheit und leichteren Verwaltung gibt es dafür zwei sehr praktische Gründe.

Erstens kann die Echtheit eines Dokuments unabhängig von der Software für E-Signaturen überprüft werden, d. h. Sie müssen sich keine Gedanken darüber machen, ob ein Verifizierungslink zu einem Server auch nach vielen Jahren noch gültig ist oder ob dann eine Fehlermeldung wie „Seite nicht gefunden“ anzeigt wird. Unabhängig davon, ob Sie ein Konto bei dem E-Signatur-Dienst haben oder ob Ihr Anbieter überhaupt noch im Geschäft ist, sind Ihre Dokumente nicht betroffen, da Sie, Ihre Kunden und andere Beteiligte nicht online gehen müssen, um das Dokument zu prüfen.

Zweitens müssen Sie das elektronisch signierte Dokument nicht bei dem E-Signatur-Dienst speichern. Das Dokument kann jedes E-Mail-, Speicher- oder Archivierungssystem sicher durchlaufen, ohne dass es beschädigt wird oder eine zusätzliche Programmierung erforderlich ist. Dadurch erhalten Sie die Flexibilität, Ihre elektronisch signierten Dokumente entsprechend Ihrer Richtlinien zur langfristigen Aufbewahrung von Dokumenten zu speichern. Mit anderen Worten kann das elektronisch signierte Dokument in einem System Ihrer Wahl indiziert, gespeichert und problemlos abgerufen werden, und Sie können sich Ihre Investitionen in diese Systeme zunutze machen.

Eine einfache Möglichkeit zur Überprüfung der Dokumentenintegrität

Wählen Sie eine intuitive Signatur- und Dokumenten-überprüfung per einfachem Mausklick. Wenn der Überprüfungsprozess zu aufwändig ist, könnten Benutzer fälschlicherweise ohne eine ordnungsgemäße Überprüfung annehmen, dass das Dokument und die Signaturen gültig sind.

> Vermeiden Sie E-Signatur-Lösungen, bei denen Sie auf einen Server zugreifen müssen, um Signaturen oder Dokumente zu überprüfen. Abgesehen vom zusätzlichen Aufwand für Benutzer, riskieren Sie auch große Probleme, wenn Sie Ihr Abonnement beenden oder der Anbieter sein Geschäft aufgibt.“

Um ein Dokument zu überprüfen, das mit der Software von OneSpan Sign elektronisch signiert wurde, klickt der Benutzer auf das Signaturfeld. Dadurch wird das Prüfprotokoll geöffnet, und sowohl die Authentifizierung des Unterzeichners als auch die Gültigkeit des Dokuments werden (wie auf Seite 5 gezeigt) automatisch überprüft.

Ein Ein-Klick-Vorgang wie dieser vereinfacht das Benutzererlebnis. Das Ergebnis: größeres Vertrauen in das E-Signatur-Verfahren und die Gewissheit, dass jegliche Fehler und betrügerische Handlungen erkannt werden. Hinzu kommt, dass geschäftliche Benutzer oder Kunden nicht in der Überprüfung von Dokumenten geschult werden müssen.

3. Sicherheit in der Cloud

Heutzutage werden E-Signatur-Lösungen sowohl lokal als auch in der Cloud angeboten. Während ein lokaler Einsatz maximale Kontrolle bietet, setzt eine wachsende Zahl von Unternehmen aller Arten und Größen auf die Cloud, und zwar aus verschiedensten Gründen, wie z. B. für eine schnelle Produkteinführung oder aus Gründen der Kosteneinsparung.

Im Fall von E-Signatur-Transaktionen, bei denen sensible Kundendaten betroffen sind, müssen bei der Nutzung eines Cloud-Dienstes zusätzlich zu den bereits erwähnten noch weitere Fragen der Sicherheit und des Datenschutzes berücksichtigt werden. Wir empfehlen dringend eine Überprüfung des Unternehmens, das Ihren E-Signatur-Dienst hostet. Welche Sicherheitsverfahren, Zertifizierungen gibt es, welche Erfolgsbilanz hat es, wie oft finden Sicherheitsprüfungen statt? Eine Prüfung der Sorgfaltspflichten rund um dessen Sicherheitsverfahren und -infrastruktur kann frühere Datenschutzverletzungen, Vorfälle von Datenverlusten/-lecks oder andere Risiken wie unzureichende Cloud- Sicherheitsexpertise aufdecken. Weitere Kriterien sind:

- die Sicherheit menschlicher Prozesse und administrativer Zugriff auf Systeme
- die Kontrollen der Sicherheits- und physischen Umgebung
- die Sicherheit der Netzwerkinfrastruktur, der Betriebssysteme und Dienste

Überprüfen Sie außerdem, ob die Plattform für E-Signaturen eine starke Datenverschlüsselung bei der Übertragung und im Ruhezustand verwendet und die Daten auf einem verschlüsselten Datenbank-Datenträger speichert, und so einen verschlüsselten Kanal für die gesamte Kommunikation gewährleistet.

Wir von OneSpan arbeiten mit führenden Cloud-Infrastrukturanbietern wie Amazon Web Services, IBM SoftLayer und Microsoft Azure zusammen. Diese Anbieter arbeiten nach bewährten Sicherheitspraktiken und erfüllen eine Reihe von gesetzlichen, branchenüblichen und IT-Standards für Sicherheit und Datenschutz, einschließlich der folgenden: ISO/IEC 27001, SOC 1/2/3, HIPAA, FIPS 140-2, FISMA und viele mehr.

Zudem setzen wir zahlreiche weitere Sicherheitsmaßnahmen auf der Anwendungsebene ein, um sicherzustellen, dass die OneSpan Sign-Plattform sicher ist und die Kundendaten geschützt werden. Als der erste und einzige Anbieter von Cloud-Lösungen für elektronische Signaturen, mit einer Zertifizierung nach Service Organization Control (SOC) 2 Typ 2, unterliegt OneSpan Sign strengsten Kontrollen.

Darüber hinaus war OneSpan Sign die erste E-Signatur-Lösung, die in einer FedRAMP-konformen Cloud, einem regierungsweiten Programm, das einen standardisierten Ansatz bei der Sicherheitsbewertung, Autorisierung und fortlaufenden Überwachung von Cloud-Produkten und -Diensten verfolgt, gehostet wurde.

Die Verfügbarkeit auf Betreiberniveau von OneSpan Sign wird durch den Einsatz mehrerer Verfügbarkeitszonen und geografischer Regionen sowie durch eine Überwachung rund um die Uhr sichergestellt (siehe OneSpan Sign

Trust Center unter support.onespan.com). Ein permanent einsatzbereiter Standort zur Notfallwiederherstellung in einer anderen geografischen Region ermöglicht eine schnelle Wiederherstellung, sollte eine Naturkatastrophe unsere Haupteinrichtungen treffen.

4. Datenresidenz

Unternehmen arbeiten zunehmend mit grenzüberschreitenden digitalen Geschäftsvorgängen und verlagern kundenbezogene Transaktionen in die Cloud. Dadurch besteht ein wachsender Bedarf sicherzustellen, dass die Daten geschützt und lokale Datenschutzvorschriften eingehalten werden. Forrester Research Inc. berichtet: „Datenresidenz wird zu einer stärkeren Anforderung werden. E-Signaturen fallen in den Anwendungsbereich von Datenschutzregeln der EU. Fachleute im Bereich S&R [Sicherheit und Risiko] müssen Datenresidenzanforderungen berücksichtigen, wenn sie Speicheroptionen von E-Signatur-Anbietern bewerten, insbesondere bei einer Speicherung in der Cloud.“[1]

Dies gilt vor allem für regulierte und auf die Einhaltung von Vorschriften ausgerichtete Branchen, die oft eine detaillierte Transparenz und Kontrolle über die Residenz von Transaktionsdaten benötigen – bis hin zur Stadt, dem Rechenzentrum und sogar der Seriennummer des Servers.

OneSpan bietet sowohl öffentliche als auch private Instanzen von OneSpan Sign in den USA, Kanada, Großbritannien, Deutschland und Australien an. Durch die Nutzung der globalen Rechenzentrumsnetzwerke unserer Technologiepartner können wir außerdem neue Instanzen von OneSpan Sign in anderen Regionen der Welt einrichten. Auf diese Weise können nicht nur die Anforderungen an die Datenresidenz im jeweiligen Land erfüllt werden, sondern Unternehmen können auch schnell ihr Geschäft weltweit skalieren und erweitern.

5. Vertrauen über den gesamten Prozess hinweg

Die Kundenerfahrung ist der Kern der digitalen Transformation. Wenn Unternehmen externe Lösungen nutzen, um ihre digitale Transformation zu unterstützen, hängt ihr Ruf meist an Maßnahmen, die außerhalb ihres Einflussbereichs liegen. Was kann ein Unternehmen also tun, um seine Marke und seinen Ruf bei der Zusammenarbeit mit externen Anbietern zu schützen?

Wir empfehlen ein White-Labeling der gesamten E-Signatur-Erfahrung, so dass Ihre Marke, und nur Ihre Marke, über die gesamte Transaktion hinweg erscheint (und nicht die Marke des

Anbieters). Dies schafft eine vertrauensvolle Beziehung zwischen Ihnen und Ihren Kunden, schützt Ihre Marke und Ihre Kunden und trägt dazu bei, die höchstmöglichen Abschlussquoten zu erzielen. Folgendes sollte Ihr Anbieter liefern können:

- Integration mit Ihren E-Mail-Servern, damit E-Mails von Ihrer Domain (z. B. @yourbank.com) aus, anstatt von der des Anbieters aus gesendet werden
- Anpassung von Farben und Logo sowie die Sichtbarkeit von Elementen wie Kopfzeile, Navigationsleiste, Fußzeile etc.
- Anpassung von Inhalt und Erscheinungsbild von E-Mail-Benachrichtigungen
- Anpassung von Dialogfenstern und Fehlermeldungen

White-Labeling als Abwehr gehen Phishing

Phishing ist eine der am weitesten verbreiteten Social-Engineering-Methoden. Beim Phishing werden Menschen dazu verleitet, auf bösartige Links in E-Mails oder SMS-Nachrichten zu klicken, um beispielsweise Malware herunterzuladen oder vertrauliche Daten an Kriminelle weiterzugeben. Angriffe durch Nachahmung von Webdiensten, einer Art Phishing-Angriff, bei dem mithilfe einer bekannte Marke über gefälschte Websites und E-Mails Menschen dazu gebracht werden, ihre Anmeldedaten an Kriminelle weiterzugeben, steigen stetig. Mit den entwendeten Anmeldedaten kann sich ein Angreifer anmelden und anstelle des Opfers agieren, und so dessen Geld stehlen – ein Problem, das noch dadurch verstärkt wird, dass Anwender gerne die gleichen Anmeldedaten für verschiedene Webdienste verwenden und Kriminelle so Zugriff auf mehrere Konten erhalten.

Es kommt immer häufiger vor, dass sich Hacker in Phishing-E-Mails an Endbenutzer als Drittanbieter ausgeben. Laut TechRepublic gehören Anbieter von Webdiensten wie Microsoft, PayPal und DocuSign zu den 10 Marken, auf die Kriminelle bei Phishing-Angriffen am häufigsten abzielen.[2] Da es sich um allgemein bekannte Marken handelt, bringen solche Phishing-Versuche hohe Klickraten ein.

Zwar ist die Multi-Faktor-Authentifizierung die beste Verteidigung gegen Hacker, die versuchen, sich unbefugten Zugang zu den Konten Ihrer Endbenutzer zu verschaffen, doch kann ein vollständiges White-Labeling Ihres E-Signatur-Workflows dazu beitragen, die Risiken von Phishing- und Nachahmungsangriffen zu minimieren. Wenn Sie eine E-Signatur-Lösung verwenden, bei der das Logo und die Marke des Anbieters ein auffälliger Teil der E-Signatur-Erfahrung sind, assoziiert der Endbenutzer Ihr Unternehmen logisch mit dem E-Signatur-Anbieter. Wenn beim Anbieter eine Sicherheits- oder Datenverletzung auftritt, kann sich dies daher auch auf Ihr Unternehmen auswirken. Darüber hinaus setzt eine Erfahrung mit der Anbietermarke Ihre Unterzeichner einem Risiko aus. Wenn einer Ihrer Kunden zum Ziel eines Phishing-Angriffs wird, so wird versucht, seine Identität und persönlichen Informationen zu stehlen. Gelingt dies, beeinträchtigt dies sein Vertrauen in Ihr Unternehmen, und er überdenkt möglicherweise seine Geschäftsbeziehung mit Ihnen.

Zwar kann White-Labeling keine Phishing-Angriffe verhindern, aber es erschwert die Machenschaften der Angreifer und reduziert damit die erfolgreichen Angriffe. Als Unternehmen für digitale Sicherheit, das bereits Milliarden von Dollar an potenziellem Betrug verhindert hat, empfehlen wir ein White-Labeling aller Aspekte der E-Signatur-Erfahrung.

Zusätzliche Überlegungen für Fachleute im Bereich Sicherheit und Risiko

Laut Forrester Research Inc. sind Fachleute im Bereich Sicherheit und Risiko (S&R) zunehmend für die Identitäts- und Zugriffsverwaltung (IAM) ihres Unternehmens verantwortlich.[3] Allzu oft verkennen S&R-Fachleute jedoch, dass die E-Signatur-Technologie mehr als nur eine Unterschrift ist, und verpassen Möglichkeiten, Einfluss darauf zu nehmen, wie E-Signaturen in das bestehende IAM-Rahmenwerk ihres Unternehmens integriert werden. S&R-Fachleute sollten sich bemühen, eine optimale digitale End-to-End-Erfahrung zu konzipieren.

Wenn Kunden sich während der digitalen Transaktion wiederholt und unnötigerweise authentifizieren müssen, beeinträchtigt dies die Qualität ihrer Erfahrung. Daher müssen S&R-Fachleute sicherstellen, dass E-Signaturen nahtlos in bestehende IAM-Lösungen integriert werden können, um umständliche Erfahrungen auf Kundenseite zu vermeiden.

Viele Finanzdienstleister und Versicherer setzen bereits Authentifizierungsdienste von Drittanbietern ein, wenn sie bei Kontoeröffnung und Neuanträgen auf Kreditdatenbanken zugreifen. Wählen Sie Lösungen, bei denen derartige Drittanbieterdienste in den Verlauf der Transaktion integriert werden können, um eine optimale Kundenerfahrung zu gewährleisten.

Fazit

Die digitale Erfahrung hat großen Einfluss auf Mitarbeiter- und Kundenerfahrung und ihr sollte darum oberste Priorität eingeräumt werden.

Sicherheit ist die Voraussetzung für vertrauenswürdige Erfahrungen. Das Thema Sicherheit muss bei elektronischen Signaturen als Ganzes betrachtet werden, von der Authentifizierung des Unterzeichners bis hin zur Unabhängigkeit vom Anbieter.

Außerdem ist es wichtig, das richtige Gleichgewicht zu finden zwischen Sicherheitsaspekten und der Benutzerfreundlichkeit einer Lösung: Vermeiden Sie, Ihre Sicherheitsanforderungen zu hoch zu schrauben, denn Ihre Geschäftsprozesse (ob auf Papier oder elektronisch) integrieren ja bereits zahlreiche Sicherheitsvorkehrungen.

Vertrauen und Sicherheit sind der Kern der digitalen Transformation. Wir bei OneSpan verfügen über mehr als 20 Jahre Erfahrung in der Bereitstellung von E-Signaturen und Authentifizierungslösungen und gewähren ein sicheres Erlebnis über alle digitalen und mobilen Kanäle hinweg. Wir können Sie bei der erfolgreichen Digitalisierung Ihrer Geschäftsprozesse begleiten und Ihren Kunden ein vertrauenswürdiges und sicheres Erlebnis bieten – unabhängig von Anwendungs fall, Kommunikationskanal oder Region.

---

[1] Forrester Research, November 12, 2015, S&R Pros Must Play An Outsized Role In Selecting And Implementing E-Signature

[2] TechRepublic https://tek.io/33T04aW

[3] Umformuliert auf Basis von Konzepten, die im Bericht vom August 2015, Forrester's Risk-Driven Identity And Access Management Process Framework behandelt wurden

OneSpan

OneSpan unterstützt Finanzinstitute und andere Organisationen, bei Ihren kühnen Vorstöße in der digitalen Transformation erfolgreich zu sein. Dies gelingt uns durch den Aufbau von Vertrauen in die Identitäten der Menschen, die von ihnen verwendeten Geräte und die Transaktionen, die ihr Leben prägen. Wir sind davon überzeugt, dass dies die Grundlage für eine verbesserte Förderung und das Wachstum des Geschäfts ist. Über 10.000 Kunden, darunter über die Hälfte der 100 weltweit führenden Banken, verlassen sich auf Lösungen von OneSpan, um ihre wichtigsten Beziehungen und Geschäftsprozesse zu schützen. Vom digitalen Onboarding über die Betrugsprävention bis hin zum Workflow-Management reduziert die einheitliche, offene Plattform von OneSpan Kosten, beschleunigt die Kundengewinnung und steigert die Kundenzufriedenheit.

KONTAKTIEREN SIE UNS
Weitere Informationen:
onespan.com/de/contact-us

Letzte Aktualisierung im September 2019.

Sicherheit für E-Signaturen and E-Transaktionen: Best Practices-Checkliste

BENUTZERIDENTITÄT, AUTHENTIFIZIERUNG UND ZUORDNUNG	
✔	Flexible Benutzeridentifizierungsverfahren: • Fernidentifizierung von Benutzern über externe Datenbanken (d. h. dynamische wissensbasierte Authentifizierung) • Fernidentifizierung von Benutzern über die Verifikation persönlicher Daten (PIV)
✔	Möglichkeit zum Hochladen von Bildern (z. B. Foto eines Führerscheins) als Teil der E-Signatur-Transaktion
✔	Flexible Benutzerauthentifizierungsverfahren: • Fernauthentifizierung von Benutzern über Benutzer-ID und Passwort • Überprüfung einer E-Mail-Adresse durch Einladung zu einer elektronischen Signatursitzung • Fernauthentifizierung von Benutzern über statische wissensbasierte Authentifizierung (d. h. geheime Authentifizierungsfragen) • Möglichkeit zur benutzerdefinierten Anpassung der Authentifizierungsfragen • Möglichkeit zur Nutzung bestehender Anmeldedaten • Möglichkeit zum umfassenden White-Labeling des E-Signatur-Vorgangs zur Verstärkung einer vertrauenswürdigen Erfahrung vom Beginn bis zum Abschluss
✔	Möglichkeit zur Konfiguration verschiedener Authentifizierungsverfahren innerhalb der gleichen Transaktion
✔	Flexibilität zur Anpassung des Authentifizierungsverfahrens an • das Risikoprofil Ihres Unternehmens • JEDEN zu automatisierenden Prozess
✔	Flexible Optionen für die persönliche Signaturzuordnung: • eidesstattliche Erklärungen bei der Übergabe • an ein persönliches Mobilgerät gesendetes SMS-Passwort (PIN)
✔	• Integration in starke Multi-Faktor-Authentifizierungslösungen (z. B. den Digipass von OneSpan)
✔	Möglichkeit zum Signieren mithilfe von Zertifikaten auf Client-Seite („qualifizierte Zertifikate“ gemäß eIDAS), die einer Einzelperson zugeordnet sind
SICHERHEIT VON DOKUMENTEN UND SIGNATUREN	
✔	Prüfprotokollinformationen müssen sicher im Dokument eingebettet sein
✔	Das Dokument und JEDE einzelne Signatur müssen mit einer digitalen Signatur abgesichert werden
✔	Ein umfassendes Prüfprotokoll sollte das Datum und die Uhrzeit JEDER einzelnen Signatur enthalten
✔	Das Prüfprotokoll muss sicher im Dokument eingebettet und mit jeder Signatur verknüpft sein
✔	Signatur- und Dokumentenüberprüfung mit nur einem Klick (z. B. die Möglichkeit, Dokumente und Signaturen offline ohne Besuch einer Website zu überprüfen)
✔	Möglichkeit zum Herunterladen einer verifizierbaren Kopie des signierten Dokuments mit dem Prüfprotokoll
CLOUD- UND DATENSICHERHEIT	
✔	Flexibilität in Bezug auf Bereitstellungsmethoden zur Einhaltung Ihrer IT- und Datensicherheitsrichtlinien • Vor-Ort-Bereitstellung • Öffentliche und private Cloud-Bereitstellung, gehostet auf weltweit führenden Cloud-Infrastrukturplattformen wie Amazon, IBM und Microsoft
✔	ISO/IEC 27001-, ISO/IEC 27017-, ISO/IEC 27018-, SOC 2- und FedRAMP-konforme E-Signatur-Lösung
✔	Veröffentlicht Sicherheitsverfahren, Zertifizierungen und die Ergebnisse von Sicherheitsprüfungen
✔	Besitzt eine konstante Erfolgsbilanz beim Schutz von Kundendaten
✔	Weltweite Rechenzentren zur Erfüllung von Anforderungen bezüglich Datenresidenz im Inland